



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/588,003	06/06/2000	Thomas Muller	367.38637X00	8997

20457 7590 12/31/2003

ANTONELLI, TERRY, STOUT & KRAUS, LLP
1300 NORTH SEVENTEENTH STREET
SUITE 1800
ARLINGTON, VA 22209-9889

EXAMINER

VAUGHAN, MICHAEL R

ART UNIT	PAPER NUMBER
----------	--------------

2131

DATE MAILED: 12/31/2003

7

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/588,003

Applicant(s)

MULLER ET AL.

Examiner

Michael R Vaughan

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 06 June 2003.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-31 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-31 is/are rejected.
- 7) ☒ Claim(s) 3,5,6,8,16,17,20,21,30 and 31 is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 06 June 2000 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
* See the attached detailed Office action for a list of the certified copies not received.
- 13) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.
a) ☐ The translation of the foreign language provisional application has been received.
- 14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) 5,6.
- 4) ☐ Interview Summary (PTO-413) Paper No(s). _____
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____

DETAILED ACTION

1. Claims 1-31 have been examined and are pending.

Information Disclosure Statement

2. An initialed and dated copy of Applicant's IDS form 1449, Paper No. 5 and 6, is attached to the instant Office action.

The information disclosure statement filed April 16, 2002 fails to comply with 37 CFR 1.98(a)(2), which requires a legible copy of each U.S. and foreign patent; each publication or that portion which caused it to be listed; and all other information or that portion which caused it to be listed. It has been placed in the application file, but the information referred to therein has not been considered.

There was no copy of reference AW provided by the applicant. For the record the examiner has retrieved a copy of the reference recited in AW and has considered it.

Claim Objections

3. Claims 3, 5, 6, 8, 30, and 31 are objected to because of the following informalities: "authorisation" and "authorising" should be --authorization-- and --authorizing--. Appropriate correction is required.

4. Claims 20 and 21 are objected to because of the following informalities: no period at the end of the sentence.

5. Claim 27 is objected to because of the following informalities: has a period at the end of line 4 instead of a semicolon.

6. Claims 16 and 17 are objected to because the trademark BLUETOOTH is used by is not capitalized.

Specification

7. The use of the trademark BLUETOOTH has been noted in this application. It should be capitalized wherever it appears and be accompanied by the generic terminology.

Although the use of trademarks is permissible in patent applications, the proprietary nature of the marks should be respected and every effort made to prevent their use in any manner which might adversely affect their validity as trademarks.

Claim Rejections - 35 USC ' 112, second paragraph

8. Claim 27 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Clarification and/or correction are required.

Claim 27 recites the limitation "the access control" in line 10. There is insufficient antecedent basis for this limitation in the claim. Claim 27, defines two access controls;

therefore, it is unclear which of the two access controls "the access control" in line 10 refers to.

Claim Rejections - 35 USC ' 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless --

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

9. Claims 1-11, 13, 18, and 28-31 are rejected under 35 U.S.C. 102(b) as being anticipated by Orita (USP 5,163,147).

As per claim 1, Orita teaches a device for communicating with other devices to allow them to access applications, comprising:

at least a first application (column 1, line 63);

Authentication means for authenticating a communicating device (column 2, lines 4-7);

access control means accessible by a communicating device requesting access to the first application without the communicating device having been authenticated by

the authentication means, and arranged to arbitrate whether access of the communicating device to the first application is granted or refused wherein if the arbitration requires an authentication of the communicating device, the access control means instructs the authentication means to authenticate the communicating device (column 1, lines 51-56 and column 2, lines 10-19).

As per claim 2, Orita teaches the access control means is arranged to store security indications in association with accessible applications, wherein the stored security indication associated with the first application is indicative of whether authentication of the communicating device is or is not required during arbitration (column 3, lines 7-9 and Fig 1).

As per claim 3, Orita teaches a user interface for authorizing access to an application during arbitration, the access control means being arranged to store security indications in association with accessible applications, wherein the stored security indication associated with the first application is indicative of whether user authorization of the communicating device is or is not required during arbitration (column 1, lines 58-59, column 3, lines 7-9, and Fig 1).

As per claim 4, Orita teaches the stored security indication associated with the first application is indicative of whether authentication of the communicating device is or

is not required during arbitration, in independence of the identity of the communicating device (column 2, lines 12-15).

As per claim 5, Orita teaches the access control means is further arranged to store trust indications in association with devices, and wherein the stored security indication associated with the first application is indicative of whether user authorization of the communicating device is or is not required during arbitration in dependence upon any stored trust indication associated with the communicating device (see Fig 1, column 1, lines 62-68 and column 3, lines 7-10).

As per claim 6, Orita teaches a user interface for authorizing access to an application during arbitration, the access control means being arranged to store trust indications in association with devices, wherein if there is a stored trust indication associated with the communicating device then no user authorization is required (column 3, lines 33-40).

As per claim 7, Orita teaches the access control means receives indications originating from communicating device identifying the communicating device (column 3, lines 10-15).

As per claim 8, Orita teaches a user interface for authorizing access to an application during arbitration, the access control means being arranged to store trust

indications in association with devices and to store security indications in association with accessible applications, wherein if there is a stored trust indication associated with the communicating device then no user authorization is required (column 3, lines 33-40) and if there is no trust indication associated with the communicating device user authorization is required in dependence on the stored security indication associated with the requested application (column 3, lines 45-49).

As per claim 9, Orita teaches wherein the access control means receives indications originating from the communicating device identifying the communicating device and the application requested (column 3, lines 10-15).

As per claim 10, Orita teaches having a device database which stores trust indications of different devices (column 1, lines 55-65 and column 5, line 67).

As per claim 11, Orita teaches a service database for storing security indications of the accessible applications (column 1, lines 60-64).

As per claim 13, Orita teaches the access control means is an/the interface with the first application (column 2, lines 5-11).

As per claim 18, Orita teaches comprising a plurality of applications and a plurality of access control means where each application has an access control means

connected to it (column 5, lines 65-67). Orita suggests that the system can be illustrated by many devices performing the functions, which he illustrates with the example of one host and one server in figure 1.

As per claim 28, Orita teaches a method of arbitrating the access of a requesting device to a service provided by a providing device comprising:

sending a request to access the service from the requesting device to the providing device (column 1, lines 57-65);

receiving the request at the providing device and passing it, without authenticating the requesting device, to an arbitration means interfacing the service (column 3, lines 19-22);

determining, in the arbitration means, whether to grant or refuse access to the first application by the requesting device, wherein if the determination requires an authentication of the requesting device, the authentication is performed during that determination and not previously (column 3, lines 7-9, lines 33-40, lines 48-51).

As per claim 29, Orita teaches the determination is made on the basis of the identity of service requested and/or the identity of the requesting device (column 3, lines 7-9 and lines 33-40, and lines 56-60).

As per claim 30, Orita teaches a device for providing services and allowing access by other devices to the provided services, comprising:

an interface for communicating with the other devices and receiving requests to access a service therefrom (column 1, lines 57-65 and column 3, lines 19-22);

arbitration means, for determining whether a requesting device communicating through the interface can access a service it has requested access to, arranged to store trust indications in association with requesting devices and arranged to receive from the interface an indication (column 3, lines 10-15), originating from the other device, identifying the other device, wherein, if the requesting device has a stored trust indication associated therewith no user authorization is required and if the requesting device has no stored trust indication associated therewith user authorization is requirable (column 3, lines 33-40, lines 48-51);

and a user interface (column 1, line 59) for providing user authorization.

As per claim 31, Orita teaches a device for providing services and allowing access by other devices to the provided services, comprising:

an interface for communicating with the other devices and receiving requests to access a service therefrom (column 1, lines 57-65 and column 3, lines 19-22);

arbitration means, for determining whether a requesting device communicating through the interface can access a service it has requested access to, arranged to store trust indications (column 3, lines 10-15) in association with requesting devices and store security indications in association with provided services and

arranged to receive from the interface indications, originating from the other device, identifying the other device and the service requested, wherein, if the requesting device has a stored trust indication associated therewith no user authorization is required (column 3, lines 20-23) and if the requesting device has no stored trust indication associated therewith user authorization is required in dependence upon the stored security indication associated with the requested service (column 3, lines 33-40, lines 48-51);

and a user interface for providing user authorization (column 1, line 59).

Claim Rejections - 35 USC ' 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

10. Claim 12 is rejected under 35 U.S.C. 103(a) as being unpatentable over Orita in view of Leveridge et al (WO 99/00958).

As per claim 12, Orita fails teaches to teach authentication comprises secret key exchange between the device and the communicating device. Leveridge et al teach a client-server system in which authentication comprises secret key exchange between the device and the communicating device (pg 3, lines 1-10). Leveridge et al uses a secret key exchange to encrypt a file being sent from one device to the next over unsecure channel so that the data cannot be simply intercepted and legible. It would be advantageous to use a secret key exchange to encrypt user credentials to prevent them from being stolen.

In view of this, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teaching of Leveridge et al within the system of Orita because it would provide a secure method for authentication.

11. Claims 14, 15, 16, 17, 20, 21,22, 23, 24, 25, and 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Orita in view of Haartsen et al (BLUETOOTH: Visions, Goals, and Architecture).

As per claims 14, 15, 16, 17, 20, 21, 22, 23, 25, and 26, Orita teaches a system in which a device communicates with a host (see Fig. 1) but does not expressly disclose having a protocol stack comprising a first layer and a second higher layer overlying the

first layer, with or without, intermediary layers, wherein the first lower layer is the authentication means and the second higher layer is part of the access control means. Haartsen et al disclose a protocol stack for a wireless network in which the application layer is the top layer on the stack and beneath the application layer is a Link Manager layer (Fig. 1) according to the proposed BLUETOOTH specification. The application layer talks to other applications (access control/security manager) and the Link Manager enforces fairness and management tasks (authentication) (pg. 3). The Link Manager also handles multiplexing of higher-level protocols (pg. 3). It is well known in the art that networks implement protocol stacks and layers communicate with similar layers using the same protocol. This of course allows different types of devices to communicate over common protocols. Haartsen et al discloses the types of wireless devices that could operate on such a communication system (pg. 1).

In view of this, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teaching of Haartsen et al within the system of Orita because Haartsen et al further defines the wireless framework in which the system of Orita can be implemented.

As per claim 24, the combined teachings of Orita and Haartsen et al inherently teach each multiplexing protocol layer, in the route of the request as it proceeds up through the protocol stack, queries the security manager which, if the requested application is not connected to the querying protocol layer, allows access of the request through the querying protocol layer to a higher multiplexing protocol layer, and, if the

requested application is connected to the querying protocol layer, performs an arbitration to grant or refuse access of the communicating device to the requested application. Haartsen et al teach the how BLUETOOTH works. Haartsen et al teach that BLUETOOTH has multiplexing layers that pass data up the protocol stack (pg. 3). Orita teaches that the requested application performs an arbitration to grant or refuse access of the communicating device to the requested application (column 1, lines 51-56 and column 2, lines 10-19). Therefore, it is inherent the protocol layers pass requests up to the application layer and should query the security manager in order to correctly deliver requests to the proper entity.

12. Claims 19 and 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Orita in view of Mashayekhi (USP 5,818,936).

As per claim 19, Orita teaches wherein any access control means is accessible by a communicating device requesting access to one of its connected applications without the communicating device having been authenticated by the authentication means, and is arranged to arbitrate whether access of the communicating device to the one connected application is granted or refused, the connected access control means instructing the authentication means to authenticate the communicating device if the arbitration requires an authentication of the communicating device (column 1, lines 51-56, column 2, lines 10-19, and column 3, lines 7-9). Orita fails to teach the plurality of access control means are arranged in a hierarch, wherein a first access control means

at the lowest level in the hierarchy provides access to at least a second access control means and access to one or both of a third access control means and an application, wherein access to each application is provided via one or more access control means including the first access control means and the application's connected access control means.

Mashayekhi teaches that plural applications each having access control identification can be arranged in a distributed authentication service to that once a user has been authenticated to the system, he/she can be authenticated to all of the other applications if he/she has the proper authority (column 5, lines 56-60 and column 6, lines 43- 59). It would be advantageous for a user in the system not to have to authenticate multiple times in order to use the applications on the system.

In view of this, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teaching of Mashayekhi within the system of Orita because it would permit a more flexible means by which a user can obtain many of the system's application without repetitive authentications.

As per claim 27, Orita teaches applications, comprising:
at least first and second applications (column 1, lines 60-63);
authentication means for authenticating a communicating device (column 2, lines 4-7);
first access control means accessible by a communicating device requesting access to the first application without the communicating device having been

authenticated by the authentication means, and arranged to arbitrate whether access of the communicating device to the first application is granted or refused wherein if the arbitration requires an authentication of the communicating device, the access control means instructs the authentication means to authenticate the communicating device(column 1, lines 51-56 and column 2, lines 10-19).

Orita fails to expressly disclose a second access control means accessible by a communicating device requesting access to the second application without the communicating device having been authenticated by the authentication means, and arranged to arbitrate whether access of the communicating device to the second application is granted or refused wherein if the arbitration requires an authentication of the communicating device, the access control means instructs the authentication means to authenticate the communicating device, wherein the first access control means is accessible by a communicating device requesting access to the second application without the communicating device having been authenticated by the authentication means, and is arranged to provide the access of the communicating device to the second access means.

Mashayekhi teaches that plural applications each having access control identification can be arranged in a distributed authentication service to that once a user has been authenticated to the system, he/she can be authenticated to all of the other applications if he/she has the proper authority (column 5, lines 56-60 and column 6, lines 43- 59). It would be advantageous for a user in the system not to have to authenticate multiple times in order to use the applications on the system.

In view of this, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teaching of Mashayekhi within the system of Orita because it would permit a more flexible means by which a user can obtain many of the system's application without repetitive authentications.

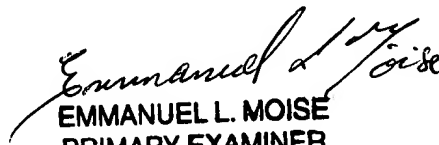
Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael R Vaughan whose telephone number is 703-305-0354. The examiner can normally be reached on M-F 7:30-4:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

MV
Michael R Vaughan
Examiner
Art Unit 2131


EMMANUEL L. MOISE
PRIMARY EXAMINER